By “ W*o*lf ”

HOW TO CRACK ANY TYPE OF CD PROTECTION:

**In this tutorial, I’m gonna show you, how to crack any type of CD Protection,
using W32Dasm, and HIEW.**

**OK, let’s start:
First of all, you have to run the damn game you want to crack, without the CD.
The game, doesn’t work of course, (Please, don’t panic) BUT a window pops up, telling you an error message.
This error message will help you to crack the game so, you’ve got to remember it.
For example: Please insert the - CD, or: You need the CD to play the - . (-, is the
game you want to crack). Anyway, if you are so idiot and you can’t remember it,
write it, in a little piece of paper.
Now, run Win32Dasm, and on the toolbar, press the first little button on the left, OR, go to Disassembler ->Open file to Disassemble. A menu will pop up. Select
the exe which you want to crack. The disassemble, will take few minutes so, I suggest you, to go for shitting.**

**OK, it finished its process.
Now, in your screen, there is a strange text, and we can’t understand anything of course. Don’t worry, the only thing we have to do, (If you want, you can change the font), is to click on the String Data References, the button next to the print button (Strn.REF).**

You can see a window which is called String Data Items. Scroll down, and try to find the game's error message. When you'll find it, double click on it, and then, close the window, to go back to the Win32Dasm text. As you can see you are somewhere in the CD check routine. This is the message's place. Now comes the interesting and difficult part, so, be careful. We don't know what all these shits mean, BUT we must know the @ offset of every call and jump command. Write down, every call and jump @ offset number. (You have to be sure, that the OPBAR change its used color to green). You need the number behind the @offset without the h. Let's go to HIEW, now.

HIEW:
To move up and down, use the cursor keys. Start HIEW. exe. In the HIEW directory, there is a list of exes and programs. Go to the directory, which you saved the game's exe, we want to crack, and click on the exe. Click F4, and then, a menu will pop up, with 3 words. Text, Hex, and Decode. Click on Decode, and now, we can understand the list of numbers. Click F5, and you can now enter the number, we wrote down, in Win32Dasm. Type it, and you will be placed at the number's place. The cursor is placed on a command.

Before I'll continue, I want to explain you something. For example, if the command where our cursor is placed on, is E92BF9BF74, means that it is 5 bytes. Every 2 numbers, are one byte: E9-2B-F9-BF-74 = 90-90-90-90-90. 10 letters, mean, 5 bytes. OK, if you understood it, you can continue.

Press F3, which means edit, and now you can edit these ten numbers. Type five times, the number 90. For every byte, 90. Now click on F10 to exit. We cracked the CD protection of the - . Congratulations.

E-mail: ia_son@hotmail.com.
ICQ: 24530541 (4 bytes).

W*o*lf
the Regulator

ENJOY!!!